Claims

What is claimed is:

1. A network security testing apparatus comprising:

a first tester that is adapted to communicably couple to a system under test;

wherein said first tester is adapted to perform a plurality of tests on the system under test;

wherein the plurality of tests includes a first test and a second test, each of which is adapted to return system environment information regarding the system under test;

wherein the first test is executed before the second test; and

wherein the first test differs from the second test in that the second test is more specific to the system under test based on information gained from the first test.

2. The network security testing apparatus of claim 1,

wherein no tests are performed on the system under test after the first test and before the second test;

wherein the time period between the first test and the second test can be negligible.

3. The network security testing apparatus of claim 1, wherein the second test is based at least partially upon system environment information detected by the first test.

4. The network security testing apparatus of claim 3, wherein the system environment information includes information regarding network connectivity from the first tester to the system under test.

5. The network security testing apparatus of claim 3, wherein the system environment information includes security obstacle information.

6. The network security testing apparatus of claim 5, wherein the security obstacle information includes session establishability information relating to an IP address used in the first test.

7. The network security testing apparatus of claim 3, further comprising:

a second tester that is adapted to communicably couple to a system under test;

wherein the first test is executed by said first tester;

wherein determination of whether the second test is executed by said first tester or by said second tester is made based at least partially upon the system environment information.

8. The network security testing apparatus of claim 3, wherein the second test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information.

9. The network security testing apparatus of claim 1, wherein said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests.

10. The network security testing apparatus of claim 2, wherein the second test is based at least partially upon system environment information detected by the first test.

11. The network security testing apparatus of claim 7, wherein the second test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information.

12. The network security testing apparatus of claim 3, wherein said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests.

13. A network security testing method comprising:

executing a first test by a first tester, wherein the first test is targeted at a system under test, and wherein the first tester is communicably coupled to the system under test;

receiving first information from the first test about the system under test, after executing the first test;

executing a second test after said receiving first information, wherein the second test is more specific to the system under test based on the first information;

receiving second information from the second test about the system under test, after executing the second test; and

wherein the second information is more specific to the system under test based on the first information.

14. The network security testing method of claim 13, wherein the time period between said executing the first test and said executing the second test can be negligible.

15. The network security testing method of claim 13, wherein said receiving first information comprises receiving system environment information.

16. The network security testing method of claim 15, wherein said receiving system environment information comprises receiving information regarding network connectivity from the first tester to the system under test.

17. The network security testing method of claim 15, wherein said receiving system environment

information comprises receiving security obstacle information.

18. The network security testing method of claim 17, wherein said receiving security obstacle information comprises receiving session establishability information relating to an IP address used in said executing the first test.

19. The network security testing method of claim 15, further comprising determining whether the second test will be executed by the first tester or by a second tester based at least partially upon the system environment information, before said executing the second test.

20. The network security testing method of claim 15, further comprising selecting the second test from a plurality of tests based at least partially upon the system environment information.

21. The network security testing method of claim 13, further comprising:

determining whether all possible information regarding the system under test has been received in light of the plurality of tests; and

executing additional tests until all possible information regarding the system under test has been received in light of the plurality of tests.

22. The network security testing method of claim 14, wherein said receiving first information comprises receiving system environment information.

23. The network security testing method of claim 19, further comprising selecting the second test from a plurality of tests based at least partially upon the system environment information.

24. The network security testing method of claim 15, further comprising:

determining whether all possible system environment information regarding the system under test has been received in light of the plurality of tests; and

executing additional tests until all possible system environment/ information regarding the system under test has been received in light of the plurality of tests.

25. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for executing a first test by a first tester, wherein the first test is targeted at a system under test, and wherein the first tester is communicably coupled to the system under test;

instructions for receiving first information from the first test about the system under test, after executing the first test;

instructions for executing a second test after receiving first information, wherein the second test is more specific to the system under test based on the first information;

instructions for receiving second information from the second test about the system under test, after executing the second test; and

wherein the second information is more specific to the system under test based on the first information.

26. The computer program product of claim 25, wherein the time period between executing the first test and executing the second test can be negligible.

27. The computer program product of claim 25, wherein receiving first information comprises receiving system environment information.

28. The computer program product of claim 27, wherein receiving system environment information comprises receiving information regarding network connectivity from the first tester to the system under test.

29. The computer program product of claim 27, wherein said receiving system environment information comprises receiving security obstacle information.

30. The computer program product of claim 29, wherein receiving security obstacle information comprises receiving session establishability information relating to an IP address used in executing the first test.

31. The computer program product of claim 27, further comprising instructions for determining whether the second test will be executed by the first tester or by a second tester based at least partially upon the system environment information.

32. The computer program product of claim 27, further comprising instructions for selecting the second test from a plurality of tests based at least partially upon the system environment information.

33. The computer program product of claim 25, further comprising:

instructions for determining whether all possible information regarding the system under test has been received in light of the plurality of tests; and

instructions for executing additional tests until all possible information regarding the system under test has been received in light of the plurality of tests.

34. The computer program product of claim 26, wherein receiving first information comprises receiving system environment information.

35. The computer program product of claim 31, further comprising instructions for selecting the second test from a plurality of tests based at least partially upon the system environment information.

36. The computer program product of claim 31, further comprising:

instructions for determining whether all possible system environment information regarding the system under test has been received in light of the plurality of tests; and

instructions for executing additional tests until all possible system environment information regarding the system under test has been received in light of the plurality of tests.

37. A network security testing apparatus comprising:

a customer profile;

a plurality of test tools;

a first tester that is adapted to communicably couple to a system under test;

wherein a selected test tool is selected from said plurality of test tools based at least partially upon said customer profile; and

wherein said first tester is adapted to execute the selected test tool so as to test the system under test.

38. The network security testing apparatus of claim 37, wherein said customer profile is determined based at least partially upon an initial mapping.

39. The network security testing apparatus of claim 37, wherein the customer profile is based at least partially on information provided by a third party.

40. The network security testing apparatus of claim 37, wherein the customer profile is at least partially produced by the method of claim 24.

41. The network security testing apparatus of claim 37, further comprising:

a second tester that is adapted to communicably couple to the system under test;

wherein determination of whether the first tester or the second tester executes the selected test tool is based at least partially upon said customer profile.

42. The network security testing apparatus of claim 41, wherein said customer profile is determined based at least partially upon an initial mapping.

43. The network security testing apparatus of claim 42, wherein the customer profile is at least partially produced by the method of claim 24.

44. A network security testing method comprising:

selecting a selected test tool from a plurality of test tools based at least partially upon a customer profile; and

executing the selected test tool by a first tester so as to test a system under test, wherein the first tester is communicably coupled to the system under test.

45. The network security testing method of claim 44, further comprising:

performing an initial mapping of the system under test; and

creating the customer profile based at least partially upon the initial mapping.

46. The network security testing method of claim 44, wherein the customer profile is based at least partially on information provided by a third party.

47. The network security testing method of claim 44, wherein the customer profile is at least partially produced by the method of claim 24.

48. The network security testing method of claim 44, further comprising selecting the first tester from a plurality of testers based at least partially upon a customer profile.

49. The network security testing method of claim 48, further comprising:

performing an initial mapping of the system under test; and

creating the customer profile based at least partially upon the initial mapping.

50. The network security testing method of claim 49, wherein the customer profile is at least partially produced by the method of claim 24.

51. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for selecting a selected test tool from a plurality of test tools based at least partially upon a customer profile; and

instructions for executing the selected test tool by a first tester so as to test a system under test, wherein the first tester is communicably coupled to the system under test.

52. The computer program product of claim 51, further comprising instructions for creating the customer profile based at least partially upon an initial mapping.

53. The computer program product of claim 51, wherein the customer profile is based at least partially on information provided by a third party.

54. The computer program product of claim 51, wherein the customer profile is at least partially produced by the method of claim 24.

55. The computer program product of claim 51, further comprising instructions for selecting the tester from a plurality of testers based at least partially upon a customer profile.

56. The computer program product of claim 53, further comprising:

instructions for performing an initial mapping of the system under test; and

instructions for creating the customer profile based at least partially upon the initial mapping.

57. The computer program product of claim 56, wherein the customer profile is at least produced by the method of claim 24.

58. A network security testing apparatus comprising:

a plurality of testers;

a customer profile;

wherein each of said plurality of testers is adapted to communicably couple to a system under test; and

wherein a test of the system under test is performed by a selected tester of said plurality of testers, the selected tester being selected from said plurality of testers based at least partially upon said customer profile.

59. The network security testing apparatus of claim 58, wherein said customer profile is determined based at least partially upon an initial mapping.

60. The network security testing apparatus of claim 58, wherein the customer profile is at least partially produced by the method of claim 24.

61. The network security testing apparatus of claim 58,

wherein said plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of said plurality of testers; and

wherein the selected tester is selected from said plurality of testers based at least partially on optimizing the load balance characteristic.

62. The network security testing apparatus of claim 58,

wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling.

63. The network security testing apparatus of claim 62, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

64. A network security testing method comprising:

selecting a selected tester from a plurality of testers based at least partially upon a customer profile; and

executing a test by the selected tester, wherein the test is targeted at a system under test, and wherein the selected tester is communicably coupled to the system under test.

65. The network security testing method of claim 64, further comprising:

performing an initial mapping of the system under test; and

creating the customer profile based at least partially upon the initial mapping.

66. The network security testing method of claim 64, wherein the customer profile is at least partially produced by the method of claim 24.

67. The network security testing method of claim 64,

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein said selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

68. The network security testing method of claim 64,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein said selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

69. The network security testing apparatus of claim 68, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

70. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for selecting a selected tester from a plurality of testers based at least partially upon a customer profile; and

instructions for executing a test by the selected tester, wherein the test is targeted at a system under test, and wherein the selected tester is communicably coupled to the system under test.

71. The computer program product of claim 70, further comprising:

instructions for performing an initial mapping of the system under test; and

instructions for creating the customer profile based at least partially upon the initial mapping.

72. The computer program product of claim 70, wherein the customer profile is at least partially produced by the method of claim 24.

73. The computer program product of claim 70,

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

74. The network security testing method of claim 70,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

75. The network security testing apparatus of claim 74, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

76. A network security testing apparatus comprising:

a first tester that is adapted to communicably couple to a system under test, wherein said first tester is adapted to perform a test on the system under test;

wherein said first tester is adapted to make a first attempt to communicably couple to the system under test before the test;

wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and

wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the system under test.

77. The network security testing apparatus of claim 76, wherein each test returns security obstacle information of the system under test.

78. The network security testing apparatus of claim 76,

wherein the first attempt is made using a first originating IP address;

wherein the second attempt is made using a second originating IP address that is essentially the same as the first originating IP address;

wherein a third attempt to communicably couple to the system under test is made using a third originating IP address that is different from the second originating IP address; and

wherein the combination of success of the first attempt, failure of the second attempt, and success of the third attempt is interpreted as a possibility including the detection; and

wherein the combination of success of the first attempt, failure of the second attempt, and failure of the third attempt is interpreted as a possibility including:

a network connectivity problem between the first tester and the system under test; and

the detection.

79. The network security testing apparatus of claim 77, further comprising:

a second tester that is adapted to communicably couple to the system under test;

wherein the combination of success of the first attempt, failure of the second attempt, and success of the third attempt is interpreted as a possibility including the detection; and

wherein the combination of success of the first attempt, failure of the second attempt, and failure of the third attempt is interpreted as a possibility including a network connectivity problem between the first tester and the system under test.

80. A network security testing method comprising:

attempting a first communicable coupling by a first tester to a system under test;

executing a test by the first tester, wherein the test is targeted at the system under test;

attempting a second communicable coupling by the first tester to the system under test; and

interpreting the combination success of the first communicable coupling and failure of the second communicable coupling as detection of the test by the system under test.

81. The network security testing method of claim 80, further comprising receiving security obstacle information of the system under test, responsively to said executing the test.

82. The network security testing method of claim 80, further comprising:

attempting a third communicable coupling to the system under test;

wherein said attempting a first communicable coupling is made using a first originating IP address;

wherein said attempting a second communicable coupling is made using a second originating IP address that is essentially the same as the first originating IP address;

wherein said attempting a third communicable coupling is made using a third originating IP address that is different from the second originating IP address;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including:

a network connectivity problem between the first tester and the system under test; and

the detection.

83. The network security testing method of claim 80, further comprising:

attempting a third communicable coupling by a second tester to the system under test;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including a network connectivity problem between the first tester and the system under test.

84. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for attempting a first communicable coupling by a first tester to a system under test;

instructions for executing a test by the first tester, wherein the test is targeted at the system under test;

instructions for attempting a second communicable coupling by the first tester to the system under test; and

instructions for interpreting the combination of success of the first communicable coupling and failure of the second communicable coupling as detection of the test by the system under test.

85. The computer program product of claim 84, further comprising instructions for receiving security obstacle information of the system under test, responsively to said executing the test.

86. The computer program product of claim 84, further comprising:

instructions for attempting a third communicable coupling to the system under test;

wherein the attempting a first communicable coupling is made using a first originating IP address;

wherein the attempting a second communicable coupling is made using a second originating IP address that is essentially the same as the first originating IP address;

wherein the attempting a third communicable coupling is made using a third originating IP address that is different from the second originating IP address;

wherein the combination of success of the attempting a first communicable coupling, failure of the attempting a second communicable coupling, and success of the attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of the attempting a first communicable coupling, failure of the attempting a second communicable coupling, and failure of the attempting a third communicable coupling is interpreted as a possibility including:

a network connectivity problem between the first tester and the system under test; and

the detection.

87. The computer program product of claim 84, further comprising:

instructions for attempting a third communicable coupling by a second tester to the system under test;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including a network connectivity problem between the first tester and the system under test.

88. A network security testing apparatus comprising:

a tester;

a test tool;

an application programming interface (API);

wherein said API is adapted to interface between said tester and said test tool, such that said test tool may be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool;

wherein said tester is adapted to be communicably coupled to a system under test; and

wherein said tester is adapted to test the system under test by execution of said test tool;

89. A network security testing method comprising:

adapting an application programming interface (API) to interface between a tester and a test tool, such that the test tool may be executed by the tester even if the outputs of the tester do not directly correspond to the inputs of the test tool, and such that the test tool may be executed by the tester even if the inputs of the tester do not directly correspond to the outputs of the test tool;

executing the test tool by the tester;

wherein the test tool is targeted at a system under test; and

wherein the tester is communicably coupled to the system under test;

90. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for adapting an application programming interface (API) to interface between a tester and a test tool, such that the test tool may be executed by the tester even if the outputs of the tester do not directly correspond to the inputs of the test tool, and such that the test tool may be executed by the tester even if the inputs of the tester do not directly correspond to the outputs of the test tool;

instructions for executing the test tool by the tester;

wherein the test tool is targeted at a system under test; and

wherein the tester is communicably coupled to the system under test;

91. A network security testing apparatus comprising:

a tester that is communicably coupled to a system under test, wherein said tester is adapted to test the system under test;

wherein said tester is adapted to execute a first test tool to test the system under test;

wherein said tester is adapted to execute a second test tool to test the system under test; and

wherein a time period of selected length is interposed between the execution of the first test tool and the execution of the second test tool during which said tester does not test the system under test.

92. The network security testing apparatus of claim 91,

wherein the selected length is of random length; and

wherein each test returns security obstacle information of the system under test.

93. A network security testing method comprising:

executing a first test tool by a tester, wherein the first test tool is targeted at a system under test, and wherein the tester is communicably coupled to the system under test;

executing a second test tool by the tester, wherein the second test tool is targeted at the system under test; and

selecting a time period of selected length to follow said executing the first test tool and precede said executing the second test tool.

94. The network security testing method of claim 93, further comprising:

receiving security obstacle information of the system under test, responsively to said executing the first test tool and responsively to said executing the second test tool;

wherein said selecting a time period of selected length comprises selecting a time period of random length.

95. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for executing a first test tool by a tester, wherein the first test tool is targeted at a system under test, and wherein the tester is communicably coupled to the system under test;

instructions for executing a second test tool by the tester, wherein the second test tool is targeted at the system under test; and

instructions for selecting a time period of selected length to follow execution of the first test tool and precede the execution of the second test tool.

96. The computer program product of claim 95, further comprising

instructions for receiving security obstacle information of the system under test, responsively to executing the first test tool and responsively to executing the second test tool;

wherein the selected length is of random length.

97. A network security testing apparatus comprising:

a plurality of testers;

a plurality of test tools;

wherein each of said plurality of testers is adapted to communicably couple to a system under test; and

wherein a random one of said plurality of test tools is executed by a random one of said plurality of testers, the random one of said plurality of test tools being executed so as to target the system under test, whereby the system under test is tested.

98. The network security testing apparatus of claim 97, wherein the random one of said plurality of test tools is adapted to return security obstacle information of the system under test, responsively to being executed.

99. A network security testing method comprising:

randomly selecting a one of a plurality of test tools;

randomly selecting a one of a plurality of testers;

executing the one of the plurality of test tools by the one of the plurality of testers;

wherein the one of the plurality of test tools is targeted at a system under test, and

wherein the one of the plurality of testers is communicably coupled to the system under test;

100. The network security testing method of claim 99, further comprising receiving security obstacle information of the system under test, responsively to said executing the one of the plurality of test tools.

101. A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for randomly selecting a one of a plurality of test tools;

instructions for randomly selecting a one of a plurality of testers;

instructions for executing the one of the plurality of test tools by the one of the plurality of testers;

wherein the one of the plurality of test tools is targeted at a system under test, and

wherein the one of the plurality of testers is communicably coupled to the system under test;

102. The computer program product of claim 101, further comprising instructions for receiving security obstacle information of the system under test, responsively to executing the one of the plurality of test tools.